Red Hat Certificate System Common Criteria Certification 8.1 Common Criteria Evaluation Release Notes

for new features, errata updates, and known issues
Edition 1

Landmann

Red Hat Certificate System Common Criteria Certification 8.1 Common Criteria Evaluation Release Notes

for new features, errata updates, and known issues
Edition 1

Landmann
rlandmann@redhat.com

Legal Notice

Abstract

These release notes contain the most accurate information on new features, known issues, and fixed bugs for Red Hat Certificate System 8.1.

Table of Contents

These release notes contain important information related to Red Hat Certificate System 8.1 that may not be currently available in the Product Manuals. New features, system requirements, installation notes, known problems, resources, and other current issues are addressed here. You should read these Release Notes in their entirety before deploying Red Hat Certificate System 8.1.

1. New Features for Red Hat Certificate System 8.1

Red Hat Certificate System 8.1 is a major release of Certificate System, and many new, contemporary features have been added and existing features have been made more robust and flexible.

1.1. Certified Common Criteria Environment

IMPORTANT

Red Hat Certificate System 8.1 is still undergoing Common Criteria evaluation.

The *Common Criteria for Information Technology Security Evaluation* is an international standard that helps to define the security aspects and secure implementations of software and hardware. To receive certification, software is evaluated for security in a defined and controlled environment with clearly delineated configuration and environment parameters. This environment is called the evaluated configuration.

Red Hat Certificate System 8.1 is Common Criteria certified at Evaluation Assurance Level 4 (EAL4). The procedure for setting up a certified environment, including configuration requirements and expectations, is detailed in the *Deployment and Installation Guide*.

NOTE

The Certificate System target of evaluation includes all of the Red Hat Certificate System subsystems, *except* for the Registration Authority. This means that an environment which must be Common Criteria certified cannot deploy an RA.

1.2. TPS Subsystem Enhancements

Numerous enhancements and new features have been added to the Token Processing (TPS) System to improve auditing and management and to simplify the user experience.

- An enhanced administrative interface which provides the ability to edit and validate configuration of the TPS, including profiles, server settings, and logs.
- New subsystem self-tests.
- An expanded list of auditable events, including new audit events for TPS server configuration changes.
- Improved audit log configuration, including new configuration parameters for the log size, logging flush interval, and rolling log files.
- Automatically shutting down the TPS server when its audit logs have hit the size limit and no rollover option is given.

1.3. Asynchronous Key Recovery

Previous versions of Red Hat Certificate System supported only synchronous key recovery. Synchronous key recovery meant that a single browser session (by the initiating agent) had to be kept open during the entire recovery process. While the initiating agent kept the session open, the other key recovery agents used a reference number to access that recovery thread.

Certificate System 8.1 introduces another option, an *asynchronous recovery*. Asynchronous recovery means that each step of the recovery process can be performed individually, without maintaining a continuous session. The initial request and each subsequent approval or rejection is stored in the DRM's internal database, under the key entry. The data for the recovery process can be retrieved even if the original browser session is closed or the DRM is shut down. This also allows agents to search for the key to recover, without using a reference number.

1.4. UI for Setting the Number of Key Recovery Agents

A certain number of DRM agents, called *key recovery agents*, must approve a key recovery request before a lost key can be recovered and a new certificate generated. This is configurable in the **`CS.cfg`** file in the ***`kra.noOfRequiredRecoveryAgents`*** parameter.

In Certificate System 8.1, a new **`General Settings`** tab has been added to the DRM Console which allows administrators to use the administrative UI to set the number of key agents required for a recovery operation.

1.5. Separate Enrollment and Publishing Environments

Part of the enrollment process includes publishing the issued certificate to any directories or files. This, essentially, closes out the initial certificate request. However, publishing a certificate to an external network can significantly slow down the issuance process, leaving the request open.

Red Hat Certificate System 8.1 introduces a *publishing queue*, which uses a different process to publish a new certificate than the request queue used to enroll the certificate. The publishing queue sets a defined, limited number of threads that publish generated certificates, rather than opening a new thread for each approved certificate and slowing down the overall processing time. The request queue is updated immediately to show that the enrollment process is complete, while the publishing queue sends the information to the publishing directory, including external LDAP directories, at the pace of the network traffic.

1.6. Client Authentication with OCSP Publishing

Starting with Red Hat Certificate System 8.1, publishing CRLs to an OCSP responder will require client authentication by default. The publishing CA must authenticate to the OCSP Manager using its subsystem certificate; this adds a layer of security to CRL publishing to ensure that no spurious or malicious CRLs are published.

Both configuration parameters for the **`CS.cfg`** file and new CA Console options have been added to enable and manage client authentication for OCSP publishing.

It is also possible to disable client authentication for publishing to an OCSP Manager by editing the OCSP Manager configuration and the publisher settings.

1.7. Different CA and Certificate LDAP Schema Elements for LDAP Publishing

A new default CA object class has been added to the LDAP schema used for LDAP publishing for CA certificates. This object class, ***`pkiCA`***, allows RFC 4523 support for the published CA entries.

The older object class, ***`certificationAuthority`***, specified by RFC 2252 and 2256, is still supported.

1.8. Generating a CRL from Cache

By default, CRLs are generated from the CA's internal database. However, revocation information can be collected as the certificates are revoked and kept in memory. This revocation information can then be used to update CRLs from memory. Bypassing the database searches that are required to generate the CRL from the internal database significantly improves performance so corresponding renewal profiles can be created for custom enrollment profiles.

1.9. Updated CRL Scheduling Mechanism

Time-based CRL schedules have been made more flexible in Certificate System 8.1. Previously, if delta CRLs were issued on a time-based schedule, then full CRLs had to be scheduled using time intervals within the same day. That is, if a delta CRL was scheduled to be issued at a given time, say 4:00 am and 8:00 pm, then the full CRL had to be scheduled within that same 24-hour period. Scheduling a multi-day CRL schedule was very difficult.

The ***ca.crl.MasterCRL.dailyUpdates*** parameter has been enhanced to allow multi-day schedules. Times in this parameter are separated by commas, and days are separated by colons. A full CRL within that schedule is marked by prepending an asterisk to the issuance time.

For example, to issue delta CRLs at 4:00am and 8:00 pm daily and then to issue a full CRL at 11:00 pm every third day, the ***ca.crl.MasterCRL.dailyUpdates*** parameter would have this value:

```
ca.crl.MasterCRL.dailyUpdates=04:00,20:00;04:00,20:00;04:00,20:00,*23:00
```

1.10. New and Updated Default Subsystem ACIs

The default access control instructions (ACIs) used by all subsystem and subsystem users have been updated for new user types, changes in subsystem connections, and subsystem enhancements.

1.11. Port Forwarding for Simpler User-Facing URLs

Each subsystem instance has multiple different service URLs that users can access. For example, the CA has six different URLs: two different SSL interfaces for end users (one for client authentication), an agent interface, two for administrator interfaces (one for the Java console), and a standard port. These default URLs have a relatively complex structure, which can make trying to navigate through multiple interfaces, with long path directories and different port numbers, difficult for both users and administrators.

Using port forwarding enhances the user experience by simplifying the URLs used to access web interfaces, while simultaneously providing more security by limiting user access to the instance. Port forwarding can reduce the user URL to a simpler format, which improves the user experience.

The *Certificate System Administrator's Guide* contains a sample script which can be adapted to provide port forwarding and simplified URLs for most environments.

IMPORTANT

For port forwarding to work, the machine must be configured to use three different IP addresses, one each for end-user, agent, and admin interfaces.

1.12. Configurable SSL Session Timeout Periods

In Red Hat Certificate System 8.1, all of the PKI subsystem instances have been given a default SSL session timeout period. This timeout removes data from the session cache when the timeout period (meaning, the inactive period) is reached, which decreases the ability of unauthorized users to access that information. This time out period can be configured in the instance's **`server.xml`** file (CA, DRM, OCSP, and TKS) or the instance's **`nss.conf`** file (RA and TPS).

1.13. Using a Java Subsystems with the Java Security Manager

All Java services have the option of having a Security Manager which defines unsafe and safe operations for applications to perform. When the Java subsystems are created, they have the Security Manager enabled automatically, meaning each Tomcat instance starts with the Security Manager running (the **`-secure`** flag is set).

Optionally, the Java Security Manager is disabled if the Java subsystem instance is created with the **`-sans_security_manager`** option.

1.14. In-Place Upgrade

Previous releases of Certificate System required a migration from one system to another, using a set of migration scripts to update certificate and internal data.

Red Hat Certificate System 8.1 allows in-place upgrades of Certificate System 8.0 instances. Two scripts are provided to update the LDAP entries and to update the UI files. This simplified procedure makes it easier to update to this newer release without migrating operating system versions or hosts.

The upgrade scripts are contained in the **`pki-migrate`** package and are located with the migration scripts in the **`/usr/share/pki/migrate/80To81/`** directory.

Upgrade procedures are described in the *Red Hat Certificate System 8.1 Migration Guide*.

Migration scripts are still available to migrate from 7.1, 7.2, and 7.3 instances on different machines.

2. Supported Platforms

This section covers the different server platforms, hardware, tokens, and software supported by Red Hat Certificate System 8.1.

2.1. Server Support

The Certificate System subsystems are supported on the following platforms:

- Red Hat Enterprise Linux 5.6 and later for x86
- Red Hat Enterprise Linux 5.6 and later for x86_64

2.1.1. Server Requirements

Table 1. Red Hat Enterprise Linux Server Requirements

Component	Details
CPU	Intel — 2.0 ZZ Pentium 4 or faster
RAM	1 GB (required)
Hard disk storage space	Total is approximately 5 GB - Total transient space required during installation: 1 GB - Hard disk storage space required for installation: - Space required to set up, configure, and run the server: approximately 2 GB - Additional space for database growth in pilot deployment: approximately 1 GB - Total disk storage space for installation: approximately 1 GB

2.1.2. Red Hat Enterprise Linux Considerations

Before installing the Certificate System packages, ensure that the proper dependencies are installed on the Red Hat Enterprise Linux system.

The following package groups and packages must be installed on all Red Hat Enterprise Linux systems:

- gnome-desktop (package group)
- compat-arch-support (package group)
- web-server (package group)
- kernel-smp (package)
- e2fsprogs (package)
- firefox (package)

On 64-bit Red Hat Enterprise Linux platforms, ensure that the 64-bit (x86_64) **compat-libstdc++** libraries are installed, and not only the 32-bit (i386) libraries. To confirm this, run the following command as **root**:

```
rpm -qi compat-libstdc++ --queryformat '%{NAME}-%{VERSION}-
%{RELEASE}.%{ARCH}.rpm\n' | grep x86_64
```

Numerous libraries should be displayed.

2.2. Client Support

The Enterprise Security Client is supported on the following platforms:

- Apple Macintosh OS X 10.5.8 and higher (Leopard) (Power PC, Intel)
- Microsoft Windows Vista 32-bit
- Microsoft Windows Vista 64-bit
- Microsoft Windows XP 32-bit
- Microsoft Windows XP 64-bit
- Red Hat Enterprise Linux 5.6 and later x86
- Red Hat Enterprise Linux 5.6 and later x86_64

2.3. Supported Web Browsers

The services pages for the subsystems require a web browser that supports SSL. It is strongly recommended that users such as agents or administrators use Mozilla Firefox to access the agent services pages. Regular users should use Mozilla Firefox or Microsoft Internet Explorer.

NOTE

The only browser that is fully-supported for the HTML-based instance configuration wizard is Mozilla Firefox.

Table 2. Supported Web Browsers by Platform

Platform	Agent Services	End User Pages
Red Hat Enterprise Linux	Firefox 3.x	Firefox 3.x
Windows Vista	Firefox 2.x	Firefox 2.x Internet Explorer 7 and higher
Windows XP	Firefox 2.x	Firefox 2.x Internet Explorer 6 and higher
Mac OS 10.5.8 and higher	Agent services are not supported for Mac	Firefox 2.x

2.4. Supported Smart Cards

The Enterprise Security Client supports Global Platform 2.01-compliant smart cards and JavaCard 2.1 or higher.

The Certificate System subsystems have been tested using the following tokens:

- Gemalto TOP IM FIPS CY2 64K token, both as a smart card and GemPCKey USB form factor key
- Safenet 330J Java smart card

Smart card testing was conducted using the SCM SCR331 CCID reader.

The only card manager applet supported with Certificate System is the CoolKey applet which ships with Red Hat Enterprise Linux 5.

2.5. Supported HSM

Red Hat Certificate System supports the Safenet Chrysalis-IT LunaSA and nCipher netHSM 2000 hardware security modules (HSM) by default. The tested and supported versions are listed in Table 3, “Tested HSM Versions for Red Hat Certificate System 8.1”. Other HSMs can be added by loading their libraries in the local machine and configuring the default configuration files after the Certificate System packages are installed, but before configuring the instances; this is described in the *Administrator's Guide*.

Table 3. Tested HSM Versions for Red Hat Certificate System 8.1

HSM	Firmware	Appliance Software	Client Software
Safenet Chrysalis-ITS LunaSA	4.5.2	3.2.4	3.2.4
nCipher netHSM 2000	2.33.60	11.10	

3. Installing Red Hat Certificate System Subsystems

The following sections contain information on the prerequisites and procedures for installing Certificate System subsystems, including basic information that you need to begin installing the packages.

Installing and configuring Certificate System 8.1 subsystems is described in more detail in the *Deployment and Installation Guide*.

3.1. Installation Notes

- Packages are non-relocatable. The Red Hat Certificate System base packages can not be installed to a user-designated location.
- Remove any installed **libsqlite** RPM files before installing the RA. The **sqlite** RPM files that ship with RA cause conflicts with those files.

3.2. Install the Required JDK

Certificate System requires Sun JDK 1.6.0. This JDK must be installed separately.

The OpenJDK can be installed by using **yum** or by downloading the packages directly from http://openjdk.java.net/install/. For example:

```
yum install java-1.6.0-openjdk
```

After installing the JDK, run **/usr/sbin/alternatives** as **root** to insure that the proper JDK is available:

```
/usr/sbin/alternatives --config java

There are 3 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
   1           /usr/lib/jvm/jre-1.4.2-gcj/bin/java
 + 2           /usr/lib/jvm/jre-1.6.0-openjdk/bin/java
*  3           /usr/lib/jvm/jre-1.6.0-sun.x86_64/bin/java
```

3.3. Verifying Red Hat Directory Server

All subsystems require access to Red Hat Directory Server 8.2 on the local machine or a remote machine. The Directory Server can be installed on Red Hat Enterprise Linux 5 32-bit or 64-bit.

Check that the Red Hat Directory Server is already installed. For example:

```
yum info redhat-ds
Installed Packages
Name        : redhat-ds
Arch        : x86_64
Version     : 8.1.0
Release     : 1.4.el5dsrv
Size        : 136M
Repo        : installed
...
```

Install and configure Red Hat Directory Server 8.2, if a directory service is not already available. For example:

```
yum install redhat-ds

setup-ds-admin.pl
```

IMPORTANT

The Certificate System SELinux policies assume that the Red Hat Directory Server is listening over the standard LDAP/LDAPS ports, 389 and 636, respectively. If the Directory Server is using non-standard ports, then edit the SELinux policy using **`semanage`** to relabel the LDAP/LDAPS ports and allow the subsystem to access the Directory Server.

Installing Red Hat Directory Server is described in more detail in the *Red Hat Directory Server Deployment and Installation Guide*.

3.4. Verifying Apache

Apache 2.x must be installed on Red Hat Enterprise Linux systems in order to install the TPS subsystem. Check that the appropriate version of Apache is installed.

```
yum info httpd
Installed Packages
Name    : httpd
Arch    : x86_64
Version: 2.2.3
Release: 1.4.el5
Size    : 2.9 M
Repo    : installed
...
```

Install Apache if it is not already available. For example:

```
yum install httpd
```

3.5. Installing mod_nss

Before installing the subsystem packages on Red Hat Enterprise Linux, first install or upgrade **`mod_nss`**. **`mod_nss`** is required for all Red Hat Certificate System packages, but is not included in the Red Hat Certificate System repositories, so make sure that the appropriate Red Hat Network channels are configured.

```
yum install mod_nss
```

3.6. Installing through yum

To install the subsystems on Red Hat Enterprise Linux 5.6 (32-bit), run a command like the following for each subsystem:

```
yum install pki-subsystem
```

subsystem can be any of the Certificate System subsystems:

- **ca** for the Certificate Manager.
- **ra** for the Registration Authority.
- **drm** for the Data Recovery Manager.
- **ocsp** for the Online Certificate Status Protocol Responder.
- **tks** for the Token Key System.
- **tps** for the Token Processing System.
- **console** for the Java console.

When the installation process is complete, a URL to access this instance is printed to the screen which gives the subsystem instances hostname, port, and a login PIN to access the configuration wizard.

```
Configuration Wizard listening on http://hostname.domainname:unsecure-
port/subsystem_type/admin/console/config/login?pin=pin
```

For example:

```
http://server.example.com:9180/ca/admin/console/config/login?
pin=Yc6EuvuY2OeezKeX7REk
```

3.7. Installing from an ISO

Red Hat Certificate System 8.1 can also be downloaded from Red Hat Network as an ISO image. This ISO image contains an **RPMS/** directory which can be used as a local yum repository.

Place that **RPMS/** directory on a web server and then configure yum to use that location as a repository. After that, install Certificate System as described in Section 3.6, “Installing through yum”.

4. Documentation for Certificate System 8.1

The Red Hat Certificate System 8.1 documentation includes a complete set of usage and management documentation for both regular users and administrators.

- *Deployment and Installation Guide* describes basic PKI concepts and gives an overview of the planning process for setting up Certificate System.

  This manual is intended for Certificate System administrators.
- *Certificate System Installation Guide* covers the installation process for all Certificate System subsystems.

  This manual is intended for Certificate System administrators.
- *Certificate System Administrator's Guide* explains all administrative functions for the Certificate System. Administrators maintain the subsystems themselves, so this manual details backend

configuration for certificate profiles, publishing, and issuing certificates and CRLs. It also covers managing subsystem settings like port numbers, users, and subsystem certificates.

This manual is intended for Certificate System administrators.

- *Certificate System Agent's Guide* describes how agents — users responsible for processing certificate requests and managing other aspects of certificate management — can use the Certificate System subsystems web services pages to process certificate requests, key recovery, OCSP requests and CRLs, and other functions.

  This manual is intended for Certificate System agents.

- *Managing Smart Cards with the Enterprise Security Client* explains how to install, configure, and use the Enterprise Security Client, the user client application for managing smart cards, user certificates, and user keys.

  This manual is intended for Certificate System administrators, agents, privileged users (such as security officers), and regular end users.

- *Using End User Services* is a quick overview of the end-user services in Certificate System, a simple way for users to learn how to access Certificate System services.

  This manual is intended for regular end users.

- *Certificate System Command-Line Tools Guide* covers the command-line scripts supplied with Red Hat Certificate System.

  This manual is intended for Certificate System administrators.

- *Certificate System Migration Guide* covers version-specific procedures for migrating from older versions of Certificate System to Red Hat Certificate System 8.1.

  This manual is intended for Certificate System administrators.

All of the latest information about Red Hat Certificate System and both current and archived documentation is available at https://www.docs.redhat.com.

5. Bugs Fixed in Certificate System 8.1

Along with the many new features and enhancements in Red Hat Certificate System 8.1, this release is also a bug fixing and maintenance release.

The following are some of the significant bugs that have been fixed in the 8.1 release of Red Hat Certificate System. The complete list of resolved issues is available in Bugzilla #445047.

Table 4. Fixed Bugs

Bug Number	Description
223314	Better log events and details have been added to the TPS logging so that the complete token lifecycle can be tracked.
223319	The CA and the TPS's token database could show different statuses for the same certificate in certain circumstances.http://brewweb.devel.redhat.com/brew/taskinfo?taskID=3960396
223336	A CA set up with ECC keys could not be cloned.
224709 645895	Supported ECC curves are now listed in the installation wizard so that they can be selected for creating subsystem certificates. These curves are also supported in the **`pkisilent`** script.
224765	The administrator certificate was not properly generated and imported during CA clone configuration.
224874	Running the BtoA command failed silently if the given certificate had an ECC signature.
234884	The Phone Home UI opened on Mac boxes for tokens which were already enrolled.
447596	The init start script could incorrectly return that the subsystem is running correctly when, in fact, no processes are running or sockets listening on the given ports.
451874	The Certificate Wizard in the Java Console did not support ECC keys.
453051 493765 499014 586681 586700 586707 537490	Certificate renewal did not work in the Java Console. A renewal request failed with a null pointer exception and could, potentially, cause a server crash.
454559	The OCSP required a request, along with the OCSP request, as part of the GET parameters or it returned a null pointer exception.
458888	When a PKCS #10 certificate was submitted through the end-entities page, an extra space was added to the name of the CRL distribution point.
461856	When using a DRM with the TPS on a netHSM

	device, any token enrollment would fail. The DRM was not able to properly perform server-side key generation, so it could not send a public/private key pair back to the TPS.
471318	Several security vulnerabilities, including unlimited use of a one-time PIN, were found in the SCEP implementation.
480821	Open the URL *http(s)://hostname:port/ca* opened the CA's **`webapps/`** directory and gave access to all the files.
488762	The HTTP TRACE method was enabled on the TPS.
492963	If multiple certificates were enrolled on a token, the Enterprise Security Client responded to enrollment problems differently depending on which certificate in the sequence has the error. Sometimes, the enrollment operation would fail, and sometimes it would report success, despite the fact that not all certificates were enrolled on the token.
494696	Creating a subordinate CA using an external CA could fail if the PKCS #7 chain contained a leaf certificate.
497931	The trust chain has to be downloaded and installed in Enterprise Security Client even if it was already installed in the browser.
501088	A certificate could not be revoked if it had the same serial number as the subordinate CA which issued it.
503838	If a CA had a failure publishing to an LDAP directory, it could not successfully publish to the directory again until the CA was restarted.
504056	Completed SCEP requests are incorrectly moved back to "begin" instead of "complete."
504061	Other subsystems, including subordinate CAs, could not be added to a security domain with an ECC CA.
504905	Renewing a smart card did not include the old encryption certificate, so previously encrypted data could not be accessed.
511990	The file signing profile was added to allow object signing.
512248	When a user was assigned a temporary token for a lost token, the TPS showed active certificates, while the CA showed revoked certificates.
512493	Client authentication did not work with pkiconsole in 8.0.
516632 539773	The agent services page could fail to update during a request approval and return a blank page, even though the request was approved and

[illegible]	the certificate was issued. If an agent attempted to re-approve the request, then multiple certificates could be issued for the same request.
518241	pkiconsole would not launch when the CA was configured with ECC.
519291	Deleting a CRL issuing point after editing it returned an internal server error.
521975	Failing to provide credentials when enrolling a token caused the Enterprise Security Client to hang.
521977	When attempting to format a token using a different UID than the token owner, the Enterprise Security Client would hang.
527322	It was not possible to configure a DRM clone using pkisilent.
531137	The process could run out of Java heap space while generating a CRL, which would prevent the CRL being updated.
533226 541011	The Enterprise Security Client returned the error 'Certificate Propagation has stopped working' on Windows 64-bit machines when an enrolled token was inserted.
533529	Attempting to log into the web configuration pages after a session timeout failed if you entered a PIN instead of passing the PIN in the URL.
536891	If the **`password.conf`** was removed and the wrong passwords are given when prompted, the subsystem restart would hang.
539781	The onlySomeReasons parameter for the CRL issuing point could be ignored.
542863	An incomplete audit signing certificate nickname was written in the **`CS.cfg`** file when the subsystem used an HSM. This meant that the subsystem could not locate the signing certificate to use to sign the audit log.
545852	The Enterprise Security Client would not recognize a Gemalto token inserted directly into a machine but it detected it fine if the token was inserted in a hub or smart card reader.
547507	If the signing certificate was outside the renewal grace period, both the signing and encryption certificates were deleted instead of the encryption certificate being renewed.
547831	If the encryption certificate was outside the renewal grace period, a new signing certificate could be renewed and would appear on the CA, but it was not loaded on the token and the old certificates are marked as active in the TPS.
548699	A subordinate CA's administrator certificate was being generated by the root CA, rather than the

	subordinate CA itself.
553815	A missing VLV index could cause the CA internal database to hang when processing queries for large CRLs.
563386	Submitting invalid PKCS #10 inputs to the caAgentServerCert profile would immediately crash the CA.
564059	On Windows, the Enterprise Security Client window could close or show an error when attempting to open the enrollment page.
564207	Only pending requests were returned in the agent services page, regardless of what search criteria were set.
574942	When there were more than 100,000 tokens in the database, processing requests on the TPS went from a few seconds to one or two minutes.
577949	When creating a clone from a clone, the original security domain master CA had to be contacted, instead of allowing a different master to be used.
579790	If there was an error when enrolling a token and the end-user could not format the token, the token was unusable and the TPS had corrupt data. A confirmation step has been added to the enrollment process; if there is an error, the enrollment is automatically re-initiated.
601299	Configuring a TPS instance did not properly update the security domain.
605382	Enrolling a token using **`tpsclient`** did not update the TPS token database, so the UI did not display the proper token status.
621339	The one-time PIN used by the SCEP server where not deleted once the enrollment was performed, so the same PIN could be used multiple times.
621350	An unauthenticated user could intercept and decrypt a one-time PIN in a SCEP request and authenticate a bogus certificate request.
621602	Clicking the 'Publishing' option in the console returned the error "You are not authorized to perform this operation."
623452	The console only displayed five extensions in the policy editor, regardless of how many extensions were really associated with the policy.
639082	The CRL distribution points extension threw an exception with the message *java.lang.ClassCastException: netscape.security.x509.Extension cannot be cast*.
640710	The SCEP implementation did not support HSMs.
649910	An auditor could be added to an administrator group.

651916	The DRM and OCSP were using the standard port to connect to the CA after configuration, instead of the secure port. This was allowed in Tomcat5 but caused an error in Tomcat6.
654906	An HTTP 500 error was returned when accessing https://my_pki_ca_server:9445/ca/admin/ca/getStatus.
661128	The TPS was using incorrect CA agent ports to handle certificate revocations.
662156	The HttpClient tool was hard-coded to handle 5000 bytes, which made it impossible to submit a CMC request with more than one requests attached.
668100	The DRM storage certificate profile incorrectly included the OCSP signing extended key usage extension.
670980	When a LunaSA HSM was running in FIPS mode, Certificate System could not configure ECC algorithms higher than SHA1withEC. Otherwise, the CA threw exceptions.
673508	The **`pkicreate`** script on a 64-bit system used the wrong library name for SafeNet LunaSA when configuring the storage token.
683581	Configuring a CA to use ECC curve-nistp521 failed with the error *signing operation failed*.
689501	The ExtJoiner tool failed to join multiple extensions.
694143	When searching for a request in the -agent services pages, the CA returned the next immediate request, rather than the specified one. For example, searching for request 13 would return request 14.
716307	There was some incorrect DER encoding for default values such as the name constraint. The DER encoding included component values equal to the element's default value, which is prohibited in the RFC standard.
718427	The CA continued running even after the audit log was full.
719007	The Key Constraint keyParameter was ignored using an ECC CA to generate ECC certs from CRMF.
735191	Each token is associated with a type, which can be one of the default categories in Certificate System or can be custom defined. If a token was changed from one type to another, the *token_type* value was not getting updated in the token database.
737218	The ext data attribute was standardized to use

	lower case values, but this caused the certificate request parser to ignore many of the request attributes.

6. Known Issues

These are known issues in the 8.1 release of Red Hat Certificate System. When available, workarounds are included.

Table 5. Known Issues

Bug Number	Description	Workaround
	If the TPS is configured to prompt for passwords and the incorrect password is given, then the TPS still starts, unlike the other subsystems which will prompt again for the password. This means that the incorrect password error is not caught and communicated to the administrator. If the incorrect password is given to the prompt for the token database, then all token operations will fail. However, the TPS will start correctly and will appear to run correctly; the problem exhibits in token operations.	If TPS commands or operations are failing inexplicably, then try restarting the TPS and re-entering the token database password.

223299	If a TKS master key is generated on a SafeNet LunaSA HSM, server-side key generation fails with the following error in the TKS debug log:
	`"can't generate key encryption key"`
	A similar message also appears in the debug log if server-side key generation is turned on:
	`"TokenServlet: key encryption key generation failed for` ***`CUID`***`"`
	CUID is the card unique ID.
		Do not use LunaSA HSMs to generate keys for the TKS subsystem.

223343	When an nCipher HSM is used for a Certificate System instance, the **`nfast`** group needs to include the user ID of the Certificate System instance process. For example, since default Certificate System instances run as **`pkiuser`**, then the **`pkiuser`** group needs to be added as a member to the **`nfast`** group, if the Certificate System group has not already been added as a member.	Add the Certificate System user, such as **`pkiuser`**, as a member of the **`nfast`** group.
223391	If there are multiple enrollment operations using the tpsclient tool when server-side key generation is enabled in the TPS, then the DRM connection can time out before the TPS can generate the keys. The tool will then return the error *Failed to generate key on server. Please check DRM.*	Edit the TPS **`CS.cfg`** configuration file and increase the timeout period for the connection to the DRM by adding the following line: `conn.drm1.timeout=25`
224837	The configuration wizard is still available even after the subsystem instance configuration is complete.	
226823	An error in the **`<Connector>`** entry in the **`server.xml`** file causes the server to start and listen on that connector port, but does not provide any services. This occurs if the system is configured to use an HSM, not the internal token.	

	If this error occurs, the Tomcat server returns a JSS configuration error: *Failed to create jss service: java.lang.SecurityException: Unable to initialize security library*	
224994	CEP currently logs any authentication failures during enrollment to the system log. These should log to the audit log.	
233024	The auto enrollment proxy configuration is not added to everyone's profile. This is typically occurs when configuring the auto enrollment proxy on Windows child domains where the local administrator does not have permission to modify the **`cn=configuration`** tree in Active Directory. The simplest workaround is to use the **`Run as ..`** option to authenticate as the primary domain controller administrator and to then try to modify the **`cn=configuration`**. This relates to the **`Populate AD`** option in AEP.	
234884	The Phone Home UI pops up for both enrolled and uninitialized tokens on RHEL4 and MAC OS X, even though the tokens contain Phone Home URLs.	Type in the Phone Home URL and proceed.
235150	The TKS sub-system start and stop scripts currently do not check that the package is installed before attempting to execute.	
236857	In the RA agent page, the RA attempts to retrieve revocation information for a certificate that the agent does not have the rights to see. This is not an issue at present and can be ignored.	
237050	There can be numerous *File does not exist* errors in the RA error logs. The administrator can safely ignore these error messages.	
237056	On the agent interface of the RA, the List Requests page displays the total number of certificate requests. On the List Certificates page, the corresponding information is missing. This will be fixed in the next release.	
237250	There is currently no facility for canceling certificate revocation. This will be added in the next release.	
237251	There is currently no option to add comments to a revocation request submitted through the RA. This is useful for agents if they are temporarily putting certificates on hold. This facility is currently only provided in the CA. It will be added to the RA in the next release.	
237305	The CA subsystem in Certificate System does not process SCEP requests that have been previously submitted. This can result in an error message similar to the following:	To avoid this situation, ensure that the Cisco router generates fresh sets of keys for SCEP enrollments.

	`1706.http-9080-Processor24 - [20/Apr/2007:05:47:23 PDT] [20] [3] CEP Enrollment: Enrollment failed: user used duplicate transaction ID.`	
237353	If the user clicks a link in the agent interface too fast and too many times, the server may return *Broken pipe: core_output_filter: writing data to the network* and terminate the SSL connection.	Re-authenticate to the agent interface.
238039	The Subject Alt Name extension in certificates that are issued using the caDirUserCert profile contain unsubstituted variables, such as **`$request.requestor_email$`**), if the profile request does not contain values available for substitution.	
238203	The TPS instance name is hard-coded in the **`CS.cfg`**. Because the instance name is hard-coded, the TPS looks for the configuration file in **`/var/lib/rhpki-tps/conf/CS.cfg`**.	If you create an instance with a name other than **`rhpki-tps`**, modify the **`/var/lib/`***tps-instance-name***`/cgi-bin/sow/cfg.pl`** file to remove the hard-coded instance name.
453051 483359	When trying to renew a subsystem certificate using the certificate wizard tool in the Java console (**`pkiconsole`**), the certificate renewal fails and the console throws a Java exception, such as *UNKNOWNEXCEPTION-java.util. MissingRessourceException: Can't find resource for bundle com.netscape.admin. certsrv.CMSAdminResources, key UNKNOWNEXCEPTION*. The console relied on the old policy framework to renew certificates, but the policy framework was replaced by a new profile framework in Certificate System 7.2. Therefore, the renewal feature in the console is broken. This is related to bug 499014.	Use the certificate wizard in the console to generate new certificates for the subsystem. Alternatively, use the CA's web services forms to renew the certificate or create a new renewal profile for the subsystem certificates.
454559	Attempting to connect to the Online Certificate Status Manager using **`wget`** or HTTP POST to send OCSP requests times out.	Use the **`OCSPClient`** tool to send status requests.
456701	The default signing algorithm used by the CA cannot be successfully changed in the CA configuration or when setting up the CA. The default is hard-coded to MD5withRSA.	
476096 489558	Due to a security concern, the Red Hat Directory Server Perl files on Sun Solaris platforms were moved from **`/opt/perl5x`** to **`/usr/lib/sparcv9/dirsec/perl5x`**. However, some Perl utilities includes with Certificate System are hard-coded to reference **`/opt/perl5x`**. This move can cause problems if users running Red Hat Certificate System upgrade their local Directory Server to Red Hat	Create symlinks to the new Perl directory. *ln -s /usr/lib/sparcv9/dirsrv/perl5x /opt/perl5x*

	Directory Server 8.1 on the same machine.	
487408	Importing the CA certificate chain during instance configuration does not work in Internet Explorer. Internet Explorer does not support processing a list of certificates in one blob.	Manually install the CA certificate chain.
491438	If the TPS server is unavailable, then the Enterprise Security Client opens a blank screen in security officer mode rather than returning an error message that the server is unreachable.	If a blank screen appears when opening the Enterprise Security Client in security officer mode, try restarting the TPS server, and then restarting the Enterprise Security Client.
498299	The ***tokendb.allowedTransitions*** parameter in the TPS configuration sets the revocation states that a token can be assigned. For example, a token can go from a valid state to a permanently lost state. The ***tokendb.allowedTransitions*** parameter can be set to allow a transition from a state where the certificates are permanently revoked back to the active state. However, the TPS will not allow a token to go from a permanently revoked state back to active. Even though those operations appear to complete successfully, the certificates on that token are still revoked.	
499014	When trying to renew a DRM certificate using the certificate wizard tool in the Java console (**pkiconsole**), the certificate renewal fails and the DRM crashes. The console relied on the old policy framework to renew certificates, but the policy framework was replaced by a new profile framework in Certificate System 7.2. Therefore, the renewal feature in the console is broken. This is related to bug 453501.	Generate and install new subsystem certificates using the certificate wizard in the console, rather than attempting to renew existing certificates.
499052	If the configured OCSP responder in the RA or TPS **nss.conf** file is not the default responder, then NSS attempts to verify the OCSP signing certificate used by the OCSP, but it instead creates an infinite loop attempting to verify the certificate status against itself.	Make sure that any OCSP responder in the RA or TPS **nss.conf** file is the default, such as the CA's internal OCSP service.
501299	Token operations can cause a large number of unindexed searches to be returned in the instance's internal Directory Server logs. An unindexed search shows up in Directory Server access logs as **notes=U**. Unindexed searches are resource-intensive and can affect performance for the Directory Server. However, most of the unindexed searches returned for Certificate System token operations are improperly labeled index searches when they are really indexed VLV searches (related to Red Hat Directory Server bug 507460). The remainder of the unindexed searches still had very low	

	etimes for the searches and should not significantly affect Certificate System performance.	

503641	Attempting to load the Certicom ECC module fails if SELinux is in enforcing mode, the default setting for Certificate System 8.1.
	`modutil`, the tool which is used to load ECC modules, requests text relocation permissions for Certicom's **`/usr/lib/libsbgse2.so`** library. This is not allowed by SELinux's enforcing mode.
		SELinux can be configured to allow **`/usr/lib/libsbgse2.so`** to have text relocation permissions, which allows the ECC module to be successfully loaded.
		1. Change the file context to **`textrel_shlib_t`**.
		`chcon -t textrel_shlib_t '/usr/lib/libsbgse2.so'`
		2. Then change the default file context files on the system so that the updated context is preserved even if the system is fully relabel.
		`semanage fcontext -a -t textrel_shlib_t '/usr/lib/libsbgse2.so'`
		3. Reload the ECC module; this should be successful.
		`modutil -dbdir /var/lib/pki-ca/alias/ -nocertdb -add certicom -libfile /usr/certicom/lib/libsbcpgse.so`

504013	Because of potential security risks, SCEP enrollment is disabled through the RA for Certificate System 8.1, and the corresponding enrollment forms have been removed.	
504088	The **`CRMFPopClient`** tool is used to submit a CRMF request to a CA, with proof of possession that the CA can verify. The CA then generates and, optionally, returns a certificate request or generates a request and archives the key (for DRM transport certificates).	Use the CA's web interface to submit the CRMF transport certificate request.

	Running the **`CRMFPopClient`** tool to generate a transport certificate request for a DRM returns the error *java.io.FileNotFoundException* when submitting the CRMF request to a CA.	

505200	nfast NetHSM tokens do not support DES keys with a bad parity. The Cisco ASA 5510 router generates DES keys that are not accepted by the nfast NetHSM, which means that SCEP enrollments fail when using an nfast HSM. The CA records errors that it failed to unwrap the key:
	`[10/Jun/2009:14:49:46][http-9180-Processor25]: failed to unwrap PKCS10 org.mozilla.jss.crypto.TokenException: Failed to unwrap key`
	`[10/Jun/2009:14:49:46][http-9180-Processor25]: handlePKIMessage exception javax.servlet.ServletException: Couldn't handle CEP request (PKCSReq) - Could not unwrap PKCS10 blob: Failed to unwrap key`
	`javax.servlet.ServletException: Couldn't handle CEP request (PKCSReq) -`
	`Could not unwrap PKCS10 blob: Failed to unwrap key`
	The NetHSM logs show an application error related to the DES key parity:
	`2009-06-29 13:41:32 [18436] t901b5792: pkcs11: 000008CD Application error: DES key parity wrong`
	`2009-06-29 13:41:32 [18436] t901b5792: pkcs11: 000008CD <    *phObject 0x00000000`
	`2009-06-29 13:41:32 [18436] t901b5792: pkcs11: 000008CD <    rv 0x00000013 (CKR_ATTRIBUTE_VALUE_INVALID)`
		Attempting to change the security assurances settings on the netHSM **will not address this issue**.
		SCEP enrollments cannot be performed on a CA using a netHSM token for key storage.

509804	Installing or migrating instances on a Safenet Chrysalis-IT LunaSA HSM could fail. SSL connections from the subsystem begin failing after a short period of time and the connection could not be re-established.	Make sure that the following line must be added to the **`/etc/Chrystoki.conf`** configuration file:
		`Misc { NetscapeCustomize=1023 ; }`
		Additionally, these two lines must be removed:
		`AppIdMajor=2;`
		`AppIdMinor=4;`

511327	Trying to set up a TPS using a Safenet Chrysalis-IT LunaSA HSM fails with an error indicating that the password to access the HSM was incorrect or that the CA was unavailable.	Safenet Chrysalis-IT LunaSA HSM tokens cannot be used to set up the TPS.
512029	If the same HSM partition is used to multiple Certificate System subsystem instances, than the instance names cannot be used more than once, even if the instances are on different hosts. If a user tries to configure a new instance with the same name (including the default options) as an existing instance, then configuration will stall at key generation with an error that the certificate subject name already exists.	When using an HSM, always use unique instance names.
512493	Client authentication to the Java console fails in Red Hat Certificate System 8.1 because the console is unable to verify the client certificate required for authentication. This means that the console cannot be configured to run over SSL.	**IMPORTANT** If CA is configured for client authentication over the admin port and that CA is a security domain manager, then **no new PKI subsystems can be configured that use that CA for its security domain**. New PKI instances register themselves to the security domain CA over the admin port but without using client authentication. If the CA requires client authentication, then the registration attempt fails. 1. Stop the server. `service pki-ca stop` 2. Open the **`CS.cfg`** file and change the ***authType*** value to the client authentication setting.

```
vim
/var/lib/pki-ca/conf/CS.cfg

authType=sslclientauth
```

3. Open the **`server.xml`** file and change the ***`clientAuth`*** value to **`true`** for the admin port, in the admin connector entry.

```
vim
/var/lib/pki-ca/conf/server.xml

....
<Connector
port="9445"
maxHttpHeaderSize="8192"

maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"

enableLookups="false"
disableUploadTimeout="true"

acceptCount="100"
scheme="https"
secure="true"

clientAuth="true"
sslProtocol="SSL"
```

4. Start the server.

```
service pki-ca
start
```

5. Configure the console.
   a. Open the user's console directory.

```
/user-directory/.redhat-idm-console
```

b. Create new security databases.

```
certutil -N
-d .
```

c. Export the administrator user certificate from your browser and save it to a **.p12** file, such as **/tmp/admin.p12**.

d. Copy the administrator user certificate **.p12** file to the console directory, and use **pk12util** to import it into the security databases.

```
cp -p
/tmp/admin.
p12 /user-
directory/.
redhat-idm-
console
# pk12util -
i
./admin.p12
-d /user-
directory/.
redhat-idm-
console
```

e. Export the 64-bit blob of the issuing CA certificate from the browser and save it to a file like **ca.crt**.

f. Import the CA certificate from the base 64-blob associated with the admin user cert.

		`certutil -A -d . -n ca -t CT,C,C -i ./ca.crt`
		6. The next time you run **`pkiconsole`**, it prompts for you to supply the security database password and admin certificate to allow client authentication.
		`pkiconsole https://server.example.com:9445/ca`

513450	The CA is missing the configuration to support the Authority Information Access extension for CRLs.	This entry can be added manually to the CA **`CS.cfg`** file. 1. Stop the CA instance. `service pki-ca stop` 2. Add the extension to the file. For example:

```
vim /var/lib/pki-ca/conf/CS.cfg

ca.crl.MasterCRL.extension.AuthorityInformationAccess.accessLocation0=http://hostname:9180/ca/ocsp
ca.crl.MasterCRL.extension.AuthorityInformationAccess.accessLocationType0=URI
ca.crl.MasterCRL.extension.AuthorityInformationAccess.accessMethod0=ocsp
ca.crl.MasterCRL.extension.AuthorityInformationAccess.class=com.netscape.cms.crl.CMSAuthInfoAccessExtension
ca.crl.MasterCRL.extension.AuthorityInformationAccess.critical=false
ca.crl.MasterCRL.extension.AuthorityInformationAccess.enable=false
ca.crl.MasterCRL.extension.AuthorityInformationAccess.numberOfAccessDescriptions=1
ca.crl.MasterCRL.extension.AuthorityInformationAccess.type=CRLExtension
```

3. Start the CA instance again.

```
service pki-ca start
```

The Authority Information Access extension is described in the CRLs extension reference chapter in the *Certificate System Administrator's Guide*.

523568	On Windows XP and Vista systems, logging into the Enterprise Security Client using LDAP authentication can fail if the password is stored using the SSHA hash and has the exclamation point (!) or dollar sign ($) characters.	The exclamation point (!) and dollar sign ($) characters must be properly escaped for a user to bind successfully to the Enterprise Security Client.
		- For the dollar sign ($) character, escape the dollar sign *when the password is created*:
		`\$`
		Then, enter only the dollar sign ($) character when logging into the Enterprise Security Client.
		- For the exclamation point (!) character, escape the character when the password is created *and* when the password is entered to log into the Enterprise Security Client.
		`\!`

616532	When attempting to recover keys, if you search for pending requests based on the key identifier and click the **`Recover`** button, it returns an error that it had a problem processing the request. The form used to submit the search request sends a malformed request, which results in an invalid X.509 certificate error.	Search for the recovery certificate by pasting in the full certificate blob in the search criteria form.
664594	After a key recovery request is approved and complete, the recovery request page should display a list of which DRM agents approved the recovery. Instead, the **`Recovery Approving Agents`** field is blank.	The recover**ing** page used by agents to approve the request is updated with the list of approving agents. That page can be referenced.
670980	You cannot generate subsystem certificates with ECC algorithms on a LunaSA HSM hardware token when FIPS mode is enabled.	
673182	ECC keys are not supported for signing audit logs. Neither the servers nor the **`AuditVerify`** tool support ECC keys for signed audit log files.	Use RSA keys for signing audit logs.
674485	If a TPS is configured to use a netHSM device as its token, it cannot use ECC keys. Otherwise, when the TPS tries to register with the security domain, it is unable to connect to the domain and the TPS configuration fails.	Use RSA keys for a TPS using a netHSM token.
678320	Resetting the password on a token with an applet upgrade operation will fail. Both the password reset operation and the applet upgrade operation fail.	Disable applet upgrade in the PIN reset profile.

679978	Some attributes in the Red Hat Directory Server database are improperly labeled with an octetstring index instead of a substring index. When cloning a DRM, this can cause the DRM to crash.	Restart the Directory Server instance after cloning a DRM.
683581	ECC is *not* supported as a key type for audit signing keys used by the subsystems. If ECC is selected for subsystem keys during subsystem configuration, then the **`Advanced`** option must be selected so that the audit signing key type can be manually set to RSA.	
693412	Using the DRM agent's page to search for pending recovery requests does not return the list of pending requests.	Search for the specific recovery request by using the reference number given when the recovery request was submitted. Searching by the reference number successfully returns the recovery request record. From there, the request can be approved by clicking the **`Grant`** button.
699456	If an administrator creates a custom log type, any modifications made to the file or to the log file configuration is *not* recorded in the audit log. This means that the log file is not secure and within the scope of a Common Criteria environment.	If you are trying to establish a Common Criteria-certified environment, do no use custom log files.

736834	When installing the *pki-ca* using **`yum`**, the installer throws errors that it could not fine the **`javamail.jar`** file.
	`"Installing     : tomcat5-common-lib 58/65`
	`/usr/bin/build-jar-repository: error: Could not find javamail Java extension for this JVM`
	`/usr/bin/build-jar-repository: error: Some specified jars were not found for this jvm".`
	The symlink from **`/usr/share/java/javamail.jar`** to **`/etc/alternatives/javamail`** is removed improperly.
		Re-install the *classpathx-mail* package:
		`yum reinstall classpathx-mail`
		After that, the *pki-ca* install will be successful.
		`yum install pki-ca`

743012	With an nfast NetHSM, a key changeover operation may fail with master key-related errors. Check the **`/var/log/pki-tks/catalina.out`** log for errors related to the master key:	1. Open a terminal, and run all commands from this same terminal session. 2. Set the environment

	`>2011-10-27 16:27:18 [32084]`
	`t40b90e4600000000: pkcs11-sam: 000008d5 Application`
	`error: Key type CKK_DES2 label "new_master"`
	`2011-10-27 16:27:18 [32084]`
	`t40b90e4600000000: pkcs11-sam: 000008d5 Application`
	`error: Insecure key being used too long after creation; set CKNFAST_OVERRIDE_SECURITY_ASSURANCES=longterm to allow`
	The errors mean that the NetHSM device thinks the master key is too old and is refusing the operation.
		variable to allow the nfast NetHSM to use old master keys:
		`export CKNFAST_OVERRIDE_SECURITY_ASSURANCES=longterm`
		3. Stop the TKS.
		`service pki-tks stop`
		4. Restart the nfast NetHSM.
		`/opt/nfast/sbin/init.d-ncipher restart`
		5. Restart the TKS.
		`service pki-tks start`
		6. Perform the key changeover.

743897	When attempting to create a clone with an SSL connection between the master and clone databases, the cloning configuration fails with the error *Failed to setup replication.*	Make sure that the standard LDAP port is enabled on the Directory Server instance while the clone is being created and configured. For secure environments, the standard LDAP port can be disabled on the master's Directory Server instance once the clone is configured.
746701	The Certicom ECC library stores some of its data in the user's home directory. However, this directory is not defined in the Certificate System SELinux file contexts, so when some operations attempt to access the ECC libraries, they are prevented. The system audit logs record SELinux AVC messages. For example:	If necessary, relabel the files to allow the appropriate SELinux context so that the subsystem processes can access the libraries. For example:

	`host=server.example.com type=AVC`
	`msg=audit(1318850911.600:1029): avc:`
	`denied  { write } for  pid=21671`
	`comm="java" name="jsmith.db" dev=sdb1`
	`ino=1140509`
	`scontext=root:system_r:pki_ca_t:s0`
	`tcontext=sys`
	`tem_u:object_r:usr_t:s0 tclass=dir`
	
	`host==server.example.com type=SYSCALL`
	`msg=audit(1318850911.600:1029):`
	`arch=c000003e syscall=2 success=no exit=-`
	`13 a0=2aaabc06c7b0 a1=241 a2=180 a3=0`
	`items=0 ppid=21471 pid=21671 auid=0 uid=17`
	`gid=17 euid`
	`=17 suid=17 fsuid=17 egid=17 sgid=17`
	`fsgid=17 tty=(none) ses=29 comm="java"`
	`exe="/usr/lib/jvm/java-1.6.0-openjdk-`
	`1.6.0.0.x86_64/jre/bin/java"`
	`subj=root:system_r:pki_ca_t:s0 key=(null)`
		`/usr/sbin/semanage`
		`fcontext -a -t`
		`pki_ca_t`
		`/home/jsmith/jsmith.db`
		
		For more information on SELinux file contexts, see the SELinux Guide.

753311	When restarting the CA, SELinux returns AVC denied error messages.	The CA restarts fine, so these errors can be ignored.
772822	The **`setpin`** command does not work if the configuration for the tool is passed in the **`setpin.conf`** configuration file.	Passing the configuration parameters directly in the command line does work. Use the command-line arguments to set the configuration rather than the **`setpin.conf`** file.

7. Copyright and Third-Party Acknowledgments

Red Hat Certificate System recognizes third-party contributions to portions of its servers and clients.

7.1. Copyrights for Portions of the Server

7.1.1. Apache Software Foundation

Red Hat Certificate System TPS subsystems require a locally-installed Apache 2.0.x HTTP server. Although a local copy of this server is generally installed as part of the operating system (with its corresponding license located in **`/usr/share/doc/`***httpd-version***`/LICENSE`**, the latest version of this server is available at http://httpd.apache.org.

Red Hat Certificate System CA, DRM, OCSP, and TKS subsystems use a locally-installed Tomcat 5.5 web server. Although an appropriate server is installed when any of these subsystems are installed, the latest version of this server is available at http://tomcat.apache.org.

Red Hat Certificate System uses many components made available from Apache.

- The XML project jars are **`crimson.jar`** and **`xalan.jar`**. These are available at http://xml.apache.org.
- The Tomcat project jar files are **`servlet.jar`** and **`jakarta-naming.jar`**. These are available at http://jakarta.apache.org/tomcat/index.html.

7.1.2. Mozilla Foundation

Red Hat Certificate System uses version 4.2 of the Java™ Security Services (JSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of and, potentially, the binary images for newer versions are available at http://www.mozilla.org/projects/security/pki/jss/index.html.

Red Hat Certificate System also uses version 4.6 of the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at http://www.mozilla.org/projects/nspr/index.html.

Additionally, Red Hat Certificate System uses version 3.11 of the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at http://www.mozilla.org/projects/security/pki/nss/index.html.

Red Hat Certificate System includes a set of compiled binaries (from NSS 3.11) of several tools from the Mozilla Project provided for the convenience of the user. This includes **`certutil`**, **`cmsutil`**, **`modutil`**, **`pk12util`**, **`signtool`**, **`signver`**, and **`ssltap`**. If any problems are found in these specific tools, the source code and build instructions for the latest version of this tool and, potentially, a binary image for other newer tools are available at

http://www.mozilla.org/projects/security/pki/nss/tools/index.html.

Red Hat Certificate System includes version 1.5 R3 of Rhino JavaScript for Java™. If any problems are found in this specific distribution, the source code and build instructions for the latest version and, potentially, a binary image are available at http://www.mozilla.org/rhino/index.html.

7.1.3. Red Hat

Red Hat Certificate System requires a complete Red Hat Directory Server 8.1 binary. The open source portion of Certificate System is available at the following URL:

https://rhn.redhat.com

7.2. Copyrights for Certificate System Clients

These are the copyrights and third-party acknowledgments for portions of Red Hat Certificate System 8.1 clients.

7.2.1. Mozilla Foundation

USE AND AVAILABILITY OF OPEN SOURCE CODE. Portions of the Product were created using source code governed by the Mozilla Public License (MPL). The source code for the portions of the Product governed by the MPL is available from http://www.mozilla.org under those licenses.

Red Hat Enterprise Security Client uses the latest version of the XULRunner cross-platform package. XULRunner is a Mozilla runtime package that can be used to bootstrap XUL+XPCOM applications that are as rich as Firefox and Thunderbird. If any problems are found in this specific distribution, the source code and build instructions for the latest versions and, potentially, a binary image are available at http://developer.mozilla.org/en/docs/XULRunner_1.8.0.1_Release_Notes.

Red Hat Enterprise Security Client also uses the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at http://www.mozilla.org/projects/nspr/index.html.

Red Hat Enterprise Security Client also uses the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at http://www.mozilla.org/projects/security/pki/nss/index.html.

7.2.2. MUSCLE Drivers, Libraries, and Modules

- MUSCLE smart card middleware and applets

  Copyright 1999-2002 David Corcoran.

  Copyright 2002 Schlumberger Network Solution.

  All rights reserved.

- MUSCLE smart card middleware and applets:

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
  2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
  3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8. Document History

Revision 1-2.400	**2013-10-31**	**Rüdiger Landmann**
Rebuild with publican 4.0.0		
Revision 1-2	**2012-07-18**	**Anthony Towns**
Rebuild for Publican 3.0		
Revision 8.1-1	**January 24, 2012**	**Ella Deon Lackey**
Adding fixed bugs and known issues lists.		
Revision 8.1-0	**June 1, 2011**	**Ella Deon Lackey**
Initial draft for Certificate System 8.1 documentation.		